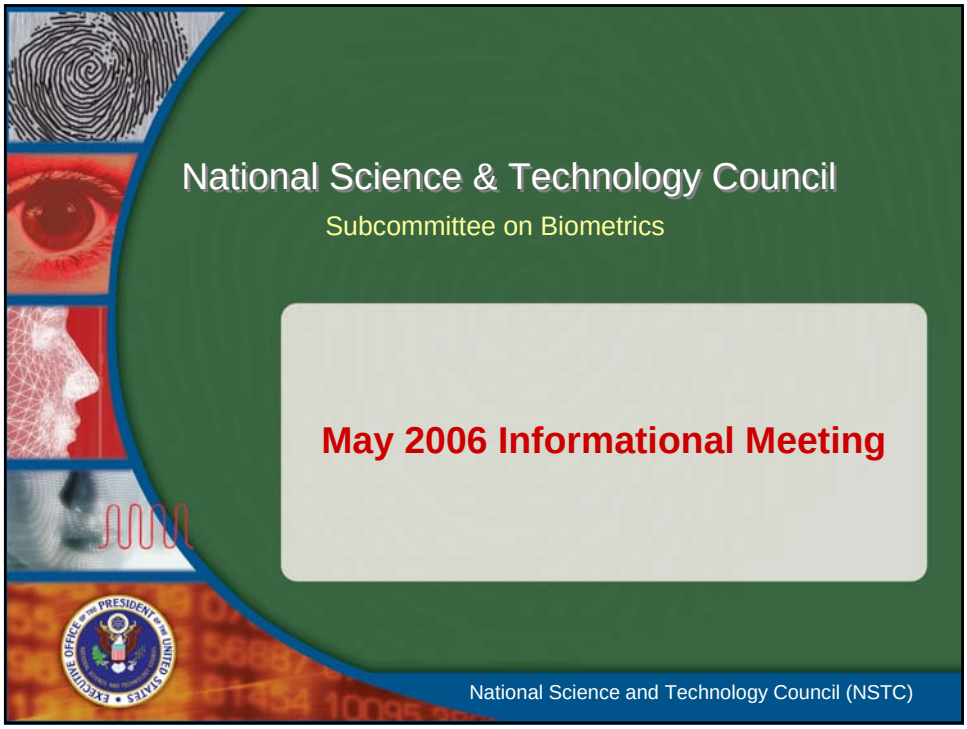
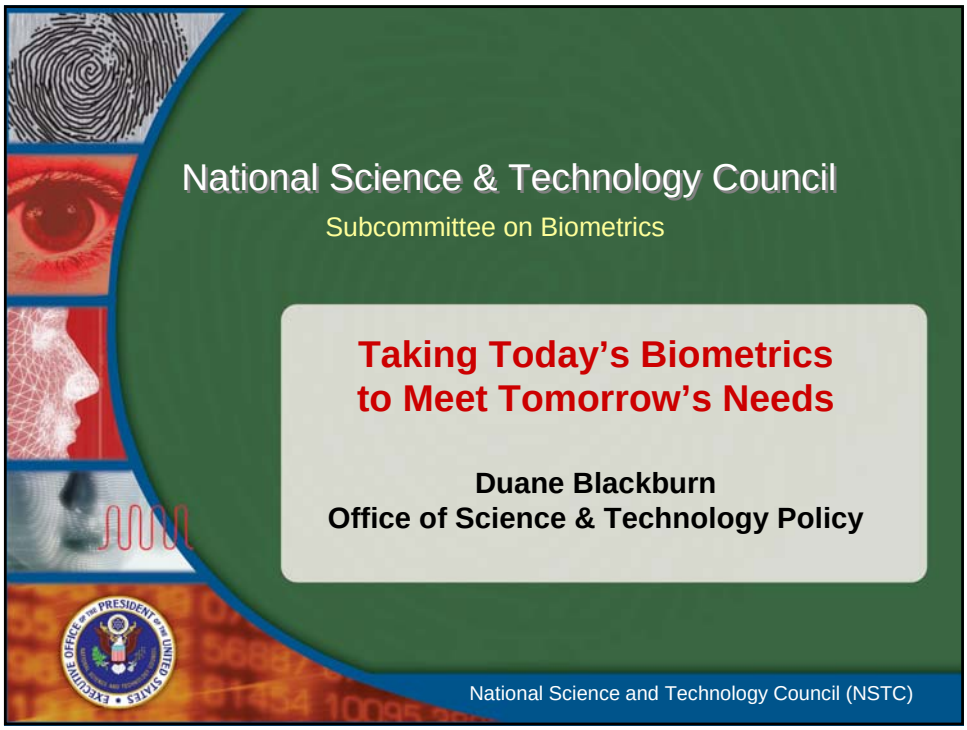
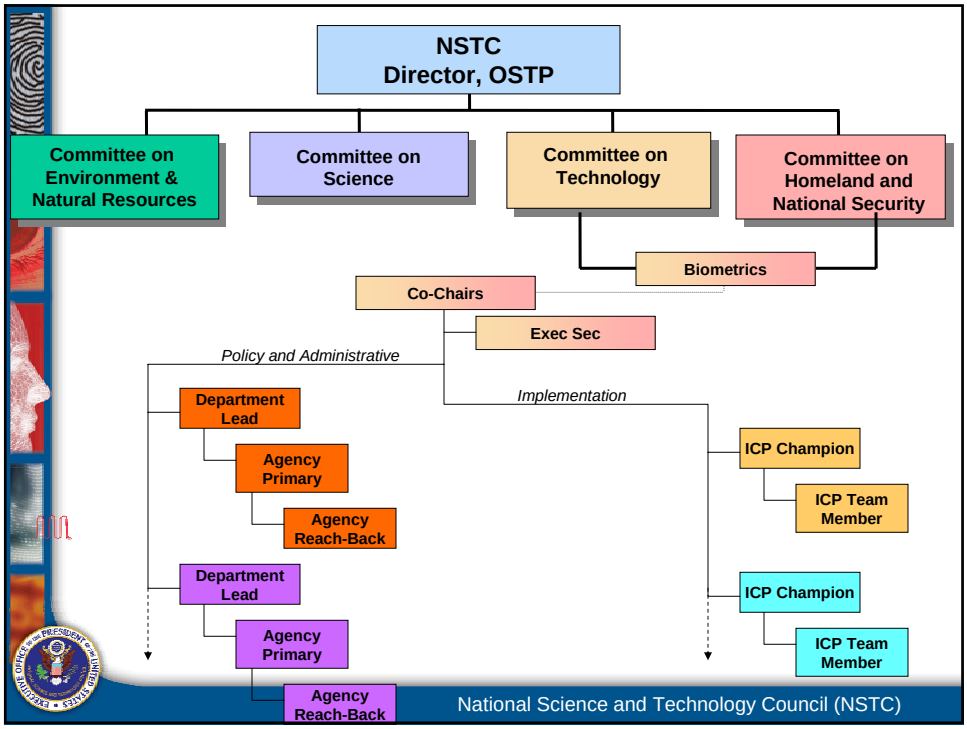
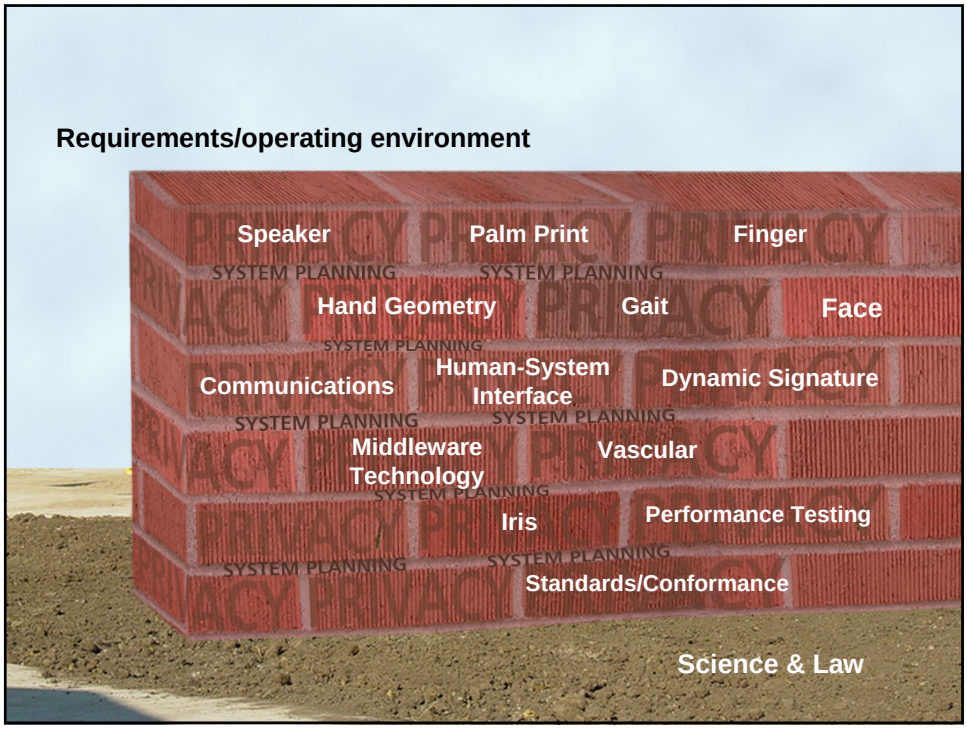

National Science & Technology Council
Subcommittee on Biometrics
May 2006 Informational Meeting
National Science and Technology Council (NSTC)


National Science & Technology Council
Subcommittee on Biometrics
Taking Today's Biometrics
to Meet Tomorrow's Needs
Duane Blackburn
Office of Science & Technology Policy
National Science and Technology Council (NSTC)



Biometrics Governance

- The combination of systems, rules and procedures that define an agreement between an individual and organization(s) regarding ownership, utilization and safeguarding of personal identity information.


Requirements/operating environment
Speaker
Palm Print
Finger
Hand Geometry
Gait
Face
Communications
Human-System Interface
Dynamic Signature
Middleware Technology
Vascular
Iris
Performance Testing
Standards/Conformance
Science & Law
SYSTEM PLANNING
PRIVACY


INTEROPERABILITY

National Science & Technology Council

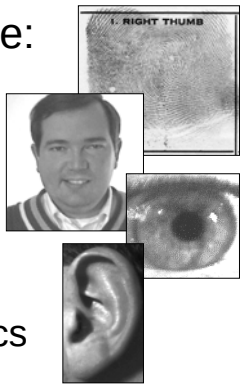
Subcommittee on Biometrics

Chris Miles
Technical Co-Chair

Department of Justice
National Institute of Justice

Advancing Technology

- NSTC Subcommittee on Biometrics works cooperatively to advance:
  - Fingerprint Recognition
  - Face Recognition
  - Iris Recognition
  - Next Generation Biometrics
  - Multi-Biometrics
  - Test and Evaluation of Biometrics



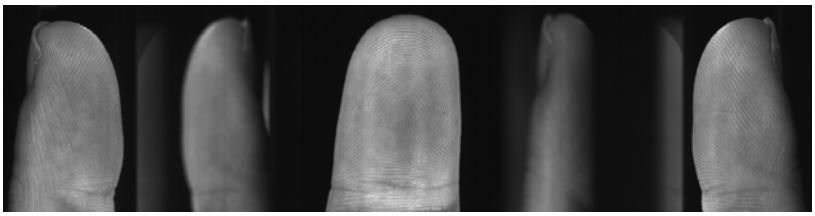
FRVT FACE RECOGNITION VENDOR TEST

FRGC FACE RECOGNITION GRAND CHALLENGE

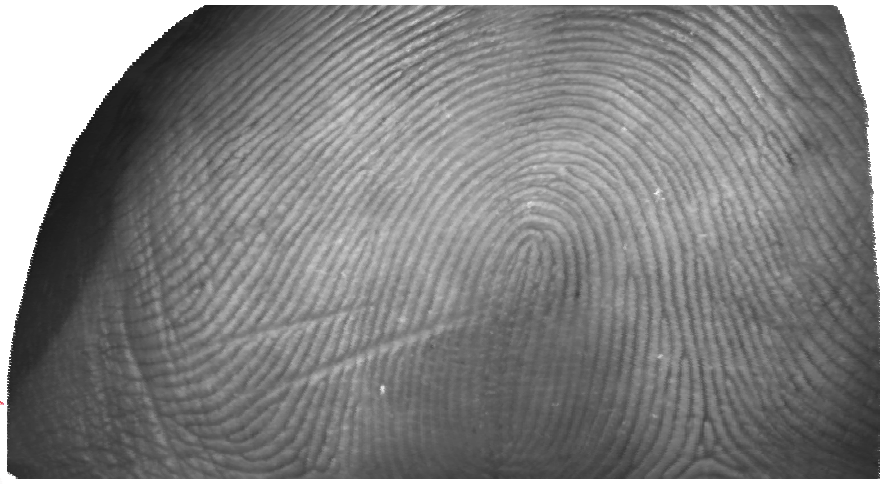
ICE IRIS CHALLENGE EVALUATION

Technology Successes

- Fast Rolled-Equivalent Fingerprints
  - Highly cooperative, joint effort of Departments of Justice, Homeland Security, Defense, and State
  - Requirements represent a major step forward in finger and palm print capture technology:
    - » Capture of 10 rolled-equivalent fingerprints in <15 seconds
    - » Capture of both palms in 1 minute or less
  - Four R&D efforts underway to produce prototype devices in 18 months to 2 years.



Technology Successes



Technology Successes

- Fast 10-print Slap Capture of Fingerprints
  - Joint Federal government user group issued an industry challenge via RFI in Sep. 2005
  - The Challenge called for industry to provide:
    - » 10-print flat capture devices and software
    - » < 6 inch x 6 inch x 6 inch size
    - » < 5 lbs. weight
    - » < 15 seconds capture time
    - » Available in < 12 months
  - Cross Match announced LScan Guardian on April 18th (received FBI certification on March 23rd)

Cross Match LScan Guardian

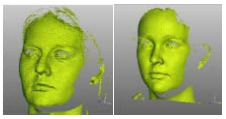
Technology Successes

- Face Recognition Grand Challenge
  - Goal is to advance still and 3D face recognition algorithm development creating an order of magnitude performance improvement
  - 17 participating organizations and 53 experiments completed
  - Best self-reported algorithms performed better than 98% verification (False Acceptance Rate = 0.001)
  - Executed by NIST. Sponsored by many USG partners

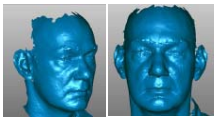
Single Still

Multiple Stills

Outdoor/ Uncontrolled



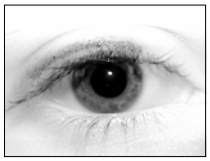
3D Single view

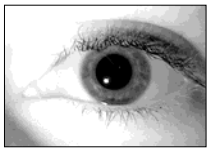


3D Full Face

Technology Successes

- Iris Challenge Evaluation
  - Goal is to facilitate iris recognition technology development and to assess iris algorithm performance
  - 9 participating organizations and 15 algorithms submitted
  - Executed by NIST. Sponsored by many USG partners
  - Best self-reported algorithms performed better than 99% verification (FAR=0.001)
  - Performance to be verified in independent assessment



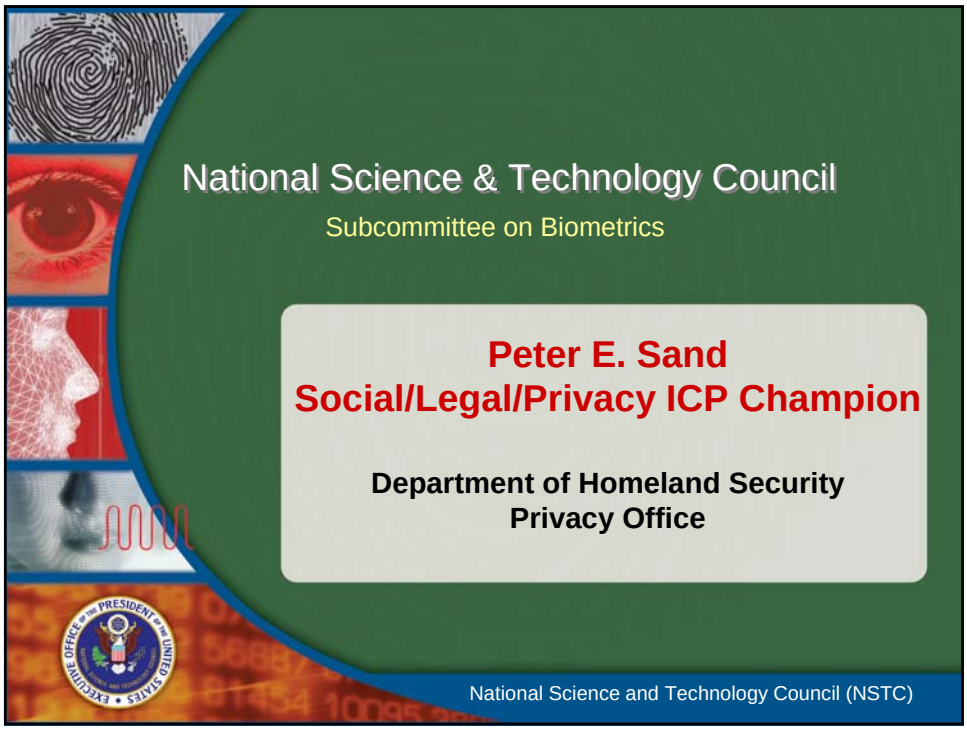


Outstanding Technology Needs

- Accelerated improvement needed:
  - Sensors to collect biometric data
  - Better performance in dynamic environments
  - Mobile or remote capture and processing
  - Biometric data quality assessment
  - Test and validation of capabilities
    - » Appropriately sized test databases
    - » Standard metrics
    - » Common evaluation criteria
    - » Product evaluations

Technology Directions

- Leadership in Test and Evaluation
  - Performance and interoperability testing
  - Continued development of metrics
  - Collection and Maintenance of Test Data
- Adoption of Interoperable Architectures
- R&D into Next Generation Biometrics
- Convergence of Forensics and Biometrics



Overview

- The Challenge: Convergence: Full Context
  - The Paper: Full Detail
  - The Framework: Application
  - The Online Resource: Ongoing Background
- The Privacy Value
- Building Functional Architecture: Privacy
- Integrated Architectures: Full Context
- The Full Value

The Privacy Value

- Removes Fears: Show Limits, Foster Acceptance
  - Collects Too Much Information
  - Inappropriate Sharing
  - Tracking
  - Reveals “New” Information
  - Physical Harm
- Informed Analysis: Unique Perspective
  - Know what you know about individuals
  - Relationship: Individual – Information: Impact
  - Trust: Enables Connections
- Polite: Respects Beliefs & Expectations

Building Functional Architecture: Privacy

- Recognize the Foundation
- Focus into Action
- Build the Architecture
- Integrate with other Architectures (biometrics)

Recognize the Foundation

- Belief in Entitlement: Acknowledge
  - Constitution: Amendments 1-5, (skip 2)
  - "Right to Privacy": Technology, Society: Pushback
- Experience the Harm: Accommodate
  - Interference
  - Embarrassment
  - Theft
- See the Variety: Adapt
  - States
  - International

Focus into Action

- Define "Privacy" – Context Dependent
  1. Decisional: Decisions individual's life/body
  2. Spatial: Physical spaces
  3. Intentional: Privacy in Public
  4. **Informational: Control over use**
- Define Standard
  - Personal Information: ANY Information that COULD be USED in ANY way to IDENTIFY an INDIVIDUAL.
  - Used Appropriately: Founded in law/policy, Clearly & Previously Articulated, Related to Initial Collection.

Build the Architecture

- Guiding Questions:
  - Is the data Personal Information?
  - Is the Personal Information Used Appropriately?
- Structured Application of Questions (generic)
  - As data changes
  - As use changes
  - As use changes the data & data changes use
  - As technology changes what is possible – new info.

Build the Architecture

1. Status: Starting Point
2. Documentation: Expectations
3. Purpose & Success: Guide
4. Data: Personal Information by Content & Intent
5. Function: Appropriate Use
6. Technology: Secondary Issues
7. Audit & Access: Verification & Participation

Integrate with Other Architectures

Biometrics

1. Collection
2. Conversion
3. Storage
4. Comparison
5. Decision

Privacy

1. Status
2. Documentation
3. Purpose & Success
4. Data
5. Function
6. Technology
7. Audit & Access

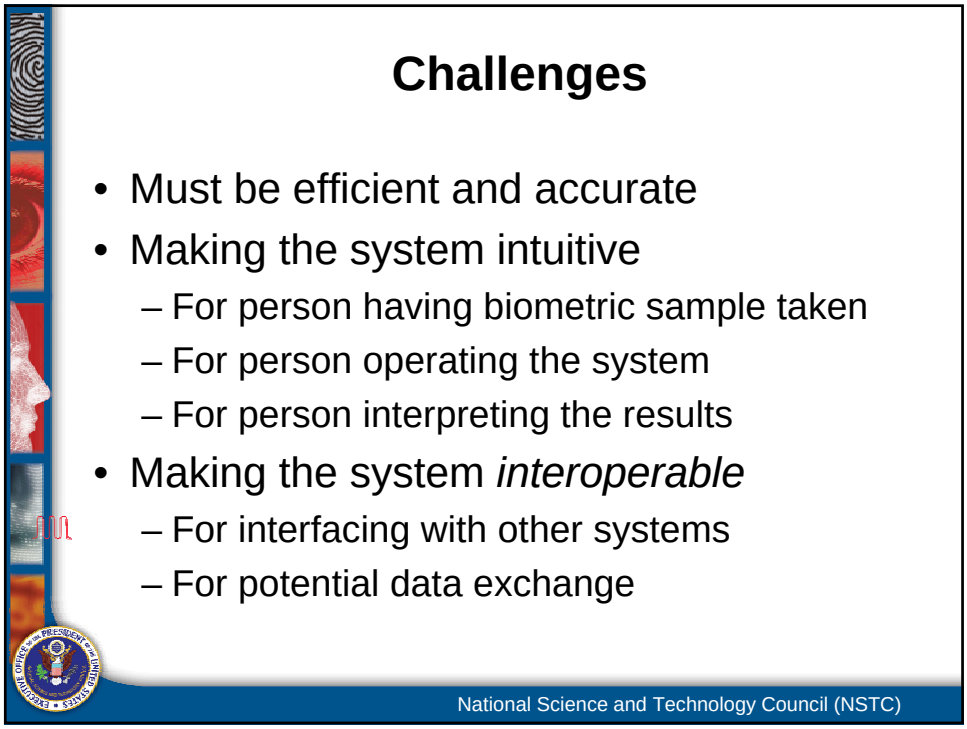
Integrate with Other Architectures

- Standard of Practice: Should, Should Not
  - Collection: Be hesitant to collect
  - Conversion: Be aware of probabilities
  - Storage: Be secure in all things
  - Comparison: Be clear of match significance
  - Decision: Be available for discussion
- Detailed Review
  - Full application of privacy framework

The Full Value

- Value of Biometrics:
  - Recognition of Individuals
- Value of Privacy
  - Respect for Individuals
- Value of Privacy-Protective Biometrics
  - Informed Operations
  - Broader Acceptance
  - The Third Win


National Science & Technology Council
Subcommittee on Biometrics
Brad Wing
Applications Co-Chair
Department of Homeland Security
US-VISIT
National Science and Technology Council (NSTC)


Challenges
• Must be efficient and accurate
• Making the system intuitive
– For person having biometric sample taken
– For person operating the system
– For person interpreting the results
• Making the system *interoperable*
– For interfacing with other systems
– For potential data exchange
National Science and Technology Council (NSTC)

What This Means

- Use of appropriate / accurate capture device *(addressed earlier)*
- Optimization of interaction with subject and operator during biometrics capture *(human factors)*
- Automated assessment of image at time of capture *(quality)*
- Protection of data integrity and upholding privacy *(standards)*
  - Transmission
  - Formation of template
  - Data compression and storage
- Maximization of matcher accuracy *(addressed earlier)*
- Presentation of results in an intuitive manner *(human factors)*
- Sharing data and/or results with other parties (when deemed proper and necessary) so that they are beneficial to the other system and its users *(interoperability)*

Successes

- Departments of State and Homeland Security sharing data and performing background checks on visa applicants
- Departments of Justice and Defense linking fingerprint systems to check records on persons detained by the military
- Departments of Justice and Homeland Security working to link US-VISIT and IAFIS, including sending prints from the FBI to US-VISIT of foreign born persons with active warrants

More Successes

- Adoption by DHS of international standards for facial images and data
- US-VISIT validation processes for e-passports from other nations
- Live test of e-passports in conjunction with 4 other nations at LAX and SFO, Sydney and Singapore
- DOJ sponsorship of Iris recognition use in a school
- Facial recognition pilot in Pinellas county, Fl.

Still More Successes

- Interagency work to define common standards and formats for the government and contractor identity card (HSPD-12)
- Improved collection techniques for biometrics in military and intelligence operations
- AND THE LIST GOES ON…..

Human and Societal Factors

- Projects underway:
  - MBARK capture of face, finger, iris data
  - US-VISIT analysis of presentation interfaces for inspectors at ports-of-entry
  - Cultural factors & accessibility
  - Ethical and Social Implications of Biometric Identification Technology *2nd International meeting*

Quality

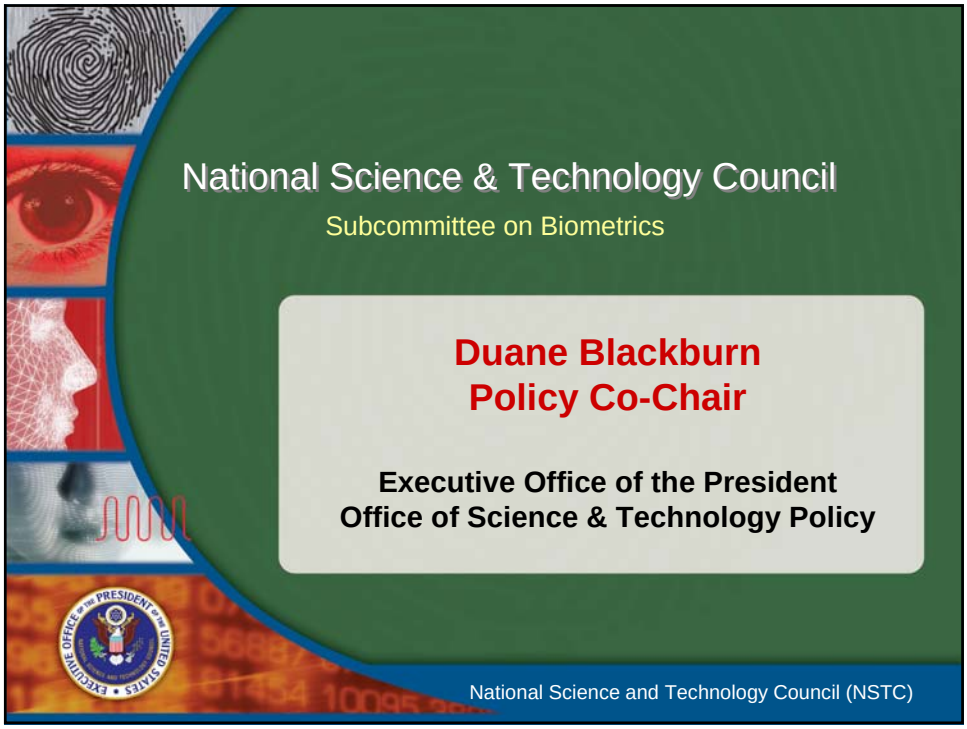
- International workshop
  - Focus on assessment at time of capture
  - Need to be predictive of matcher functionality
  - Involvement with operator vs. fully automatic
  - Quick and integrated with capture device
- National and International Standards Groups
  - Quality measure included in record headers
  - Notation as to quality analyzer used
  - Common interpretation of what the metric means

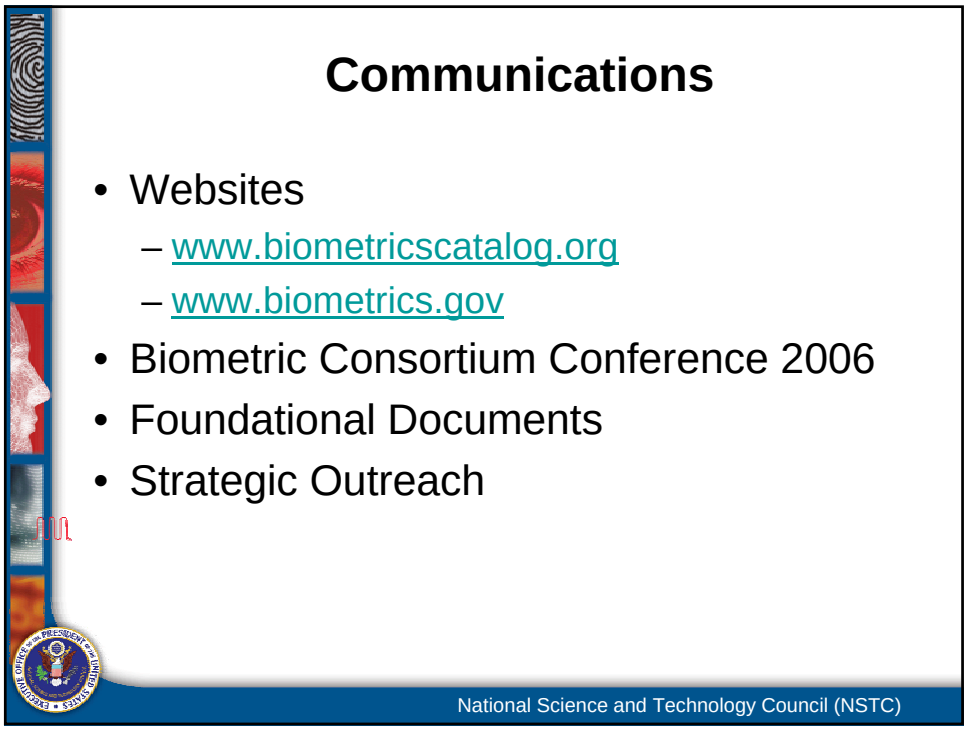
Standards

- Coordinate Government position on proposed standards
  - National
  - International
- Adopt biometric standards across the USG
- Determine 'Gaps' not met
  - i.e. Web-based biometric interfaces

Interoperability

- US-VISIT, DOD, NCIC and FBI biometric databases
- Unique Identity project for DHS systems
- Data Exchanges (Domestic/International)
  - Policies (limits on use, etc.)
  - Mechanisms
  - Ownership and responsibilities (updates/deletions…)
- Conformance Testing (to standards such as the FBI's EFTS, ANSI and ISO biometric standards, ICAO e-passport standards, etc.)
- Performance Testing
- Communication among agencies


National Science & Technology Council
Subcommittee on Biometrics
Duane Blackburn
Policy Co-Chair
Executive Office of the President
Office of Science & Technology Policy
National Science and Technology Council (NSTC)


Communications
• Websites
– www.biometricscatalog.org
– www.biometrics.gov
• Biometric Consortium Conference 2006
• Foundational Documents
• Strategic Outreach
National Science and Technology Council (NSTC)

Subcommittee Coordination Areas

- Fingerprint Recognition ICP (Miles/NIJ)
- Face Recognition ICP (Phillips/NIST)
- Iris Recognition ICP (Lively/DHS S&T)
- Multi-biometrics ICP (Grother/NIST)
- Next Generation Biometrics ICP (Swann/FBI)
- Test and Evaluation ICP (Cava/DoD BFC and Newton/NIST)

Technical Co-Chair
Miles/NIJ

- Human-System Interface ICP (Wing/US-VISIT)
- Middleware ICP (Wing/US-VISIT)
- Standards ICP (Guzman/BMO)
- Large System Updates/Integration

Applications Co-Chair
Wing/US-VISIT

- Social/Legal/Privacy ICP (Sand/DHS Privacy)
- Communications ICP (Weissman/US-VISIT)
- Research Agenda (Hogan/NIST and Dennis/DHS S&T)

Policy Co-Chair
Blackburn/OSTP